REMARKS

Reconsideration and allowance of the subject patent application are respectfully requested.

Claims 1, 2, 5-8 and 11-16 were rejected under 35 U.S.C. Section 101 as allegedly being directed to non-statutory subject matter. While not acquiescing in this rejection, method claim 7 has been amended to require storing the determination that the file is likely to be not malware, is likely to be malware or is of unknown status. Consequently, Applicant respectfully submits that claim 7 and its dependent claims 8, 11 and 12 are directed to statutory subject matter. With respect to independent claims 1 and 13 and the claims that depend therefrom, these are system claims comprising structural elements and are clearly directed to statutory subject matter. Indeed, the text on page 4 of the office action on which the Section 101 rejection is predicated is expressly directed to process claims and does not constitute a proper basis for rejecting the pending system claims. Consequently, reconsideration of the Section 101 rejection with respect to these system claims is respectfully submitted.

Claims 1, 2, 5-8 and 11-16 were rejected under 35 U.S.C. 112, second paragraph, as allegedly being indefinite due to the use of the word "likely".

Applicant traverses this rejection because the word "likely" is used merely to define the meaning of the signal which is output, not the nature of the signal itself. It is a label used to name and distinguish between the three possible signals, i.e., one signal indicates that the file is "likely to be malware", one signal indicates that the file is "not likely to be malware" and the final signal indicates that the file is "of unknown status". The independent claims are clear and comply with 35 USC Section 112, second paragraph, because they (1) unambiguously specify the circumstances in which each of the three different signals are output, e.g., if the determination in the previous phase is that the known file is "an unchanged version of a known file", "a known version of a known file" or "not determined as being an instance of a known file", and (2) the meanings of the three signals are different.

With reference to the non-limiting, illustrative embodiments, the word "likely" is perhaps clearer than referring to the signal indicating that the file "is malware" or "is not malware", because the test is heuristic not deterministic. For example, if the file is a changed version of a known file, then there is a likelihood that the file is malware but not a certainty because the file could have been changed for legitimate reasons. Indeed this is generally true of anti-malware scanning. Even signature-based virus detection can produce a false positive. There are many documented examples of clean files being reported as malware because of an accidental signature match. Therefore, those skilled in the art well understand that outputs of malware scanning indicate the file as being likely clean or likely malware, without 100% certainty.

Consequently, withdrawal of the Section 112, second paragraph, rejection is respectfully requested.

Claim 1-5, 7-11 and 13-15[1] were rejected under 35 USC Section 102(e) as allegedly being anticipated by US-2004/0088570 (Roberts). This rejection is respectfully traversed because Roberts fails to disclose each and every element of the claims as required by 35 U.S.C. Section 102(e).

For convenience the following comments are made specifically with respect to claim 1. However, equivalent comments apply to the other independent claims 7 and 13 which include corresponding features.

As previously discussed, the subject matter of the pending claims is fundamentally different from the system described in Roberts. By way of background, the non-limiting example embodiments described in the subject patent application relate to scanning files transferred through a network for malware and, in particular, to improving the detection of malware. See, e.g., page 1, lines 14-22 of the subject patent application. The non-limiting example embodiments can also reduce the load on the scanning system. See, e.g., page 1, lines 22-25 of the subject patent application. In the general case of scanning

[1] Applicant notes that claims 3, 4, 9, 10 have previously been canceled without prejudice or disclaimer.

files transferred through a network, the amount of traffic is typically enormous and the burden of scanning is very significant indeed.

The example embodiments can provide improved scanning and reduce the scanning load based on a recognition that a significant proportion of network traffic consists of executable files which are uninfected copies of common applications and utilities. See, e.g., page 2, lines 13-16 of the subject patent application. Claims 1 and 7 implement a technique that allows files to be reliably recognized as such.

In particular, this involves a file recongiser (claim 1) or corresponding method step (claim 7) which determines "whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances." This allows the file itself to be recognised. If recognised, a difference checker (claim 1) or corresponding method step (claim 7) checks "whether the file is an unchanged version of that known program."

As a result, a file which is recognised can be signaled to be not malware if it is an unchanged version or signaled to be malware if it is a changed version. This allows positive detection of new malware in an executable program even before there has been sufficient time to develop signature-based malware detection. This is significant in the context of, for example, the rapidly changing environment of the internet.

Furthermore, a definitive positive or negative result of whether the file being transferred is or is not malware can be provided based on the simple recognising and difference checking steps without the need for a full malware scan which would require a significantly higher processing load. In this way, the load on the scanning system is reduced. This reduction is significant is the context of scanning files transferred through a network which has a high volume of traffic.

In contrast to this case of scanning files transferred through a network, Roberts is concerned with a specific case of scanning web pages passed through a firewall to implement internet browsing. Paragraph [0033] of Roberts discloses that internet

addresses are identified within objects such as e-mails or files passing through the firewall. The system preemptively scans the web pages located at the identified address for malware. Paragraph [0032] discloses that the malware scanning uses "conventional techniques" and no detailed explanation is provided.

As described in paragraph [0034] of Roberts, in the event that no malware is found in the web page, the system stores the internet address in a database, together with data identifying the version of the web page including a checksum. Thus, the database stores records of internet addresses in respect of which the web page at the address has been found to be not malware in the preemptive scan.

Paragraph [0036] discloses the processing performed when a user subsequently makes an access request for the web page at an internet address. In particular, the system checks whether the internet address is stored in the database. If not, then the web page at the address is scanned for malware. But if the internet address is stored in the database, paragraphs [0037] and [0038] describe that the system checks whether the web page at the address has changed since the preemptive scan. One described technique for doing this is to compare the checksum in the database with the new checksum for the retrieved page. If the web page has not changed, then the system supplies the web page to the user.

The purpose of the system of Roberts described for example in paragraph [0010] is to reduce the delay experienced by the user after making an access request for the web page at an internet address, e.g., by clicking on the internet address. The delay is reduced because the preemptive scan avoids the need to scan the web page again at the time the access request is made, provided the web page is unchanged. Thus, the purpose of Roberts is to speed up internet browsing.

Claim 1 recites scanning of a "file being transferred between computers". Applicant and the Examiner appear to have a common understanding that this recitation corresponds in Roberts to the webpage at the internet address specified in an access request by a user, e.g., by clicking on the internet address when browsing.

However Applicant respectfully disagrees that features (a) to (c) can be read onto Roberts. In fact, Applicant submits that there are several points of novelty. These points will be separately discussed, noting that any one of these points is by itself sufficient to overcome the rejection.

A first point of novelty is the recitation in feature (a) of "a computer database containing records of known executable programs..." Applicant and the Examiner appear to have a common understanding that Roberts discloses in paragraph [00340], lines 1-7, the storage of a database of internet addresses of web pages which have been preemptively scanned and found not to contain malware, together with a checksum for each database. The Examiner contends that this disclosure of Roberts reads onto feature (a) of claim 1, but Applicant respectfully disagrees for the following reasons.

In the prior response, Applicant pointed out that a web page is not in the general case an executable program. In the Response to Arguments of the present Office Action, the Examiner purports to counter this argument by pointing out that Roberts discloses detection of malware which may be a virus which is an executable program. The Applicant accepts this disclosure is present in Roberts, but it does not follow that a lack of novelty of feature (a) is made out.

To the contrary, the Examiner is relying on the disclosure in paragraph [00340], lines 1-7 of the storage of a database of internet addresses of web pages which have been preemptively scanned and found not to contain malware. This database in Roberts therefore contains internet addresses that do not contain malware. So it follows logically from the Examiner's reliance on the malware as constituting the feature of an executable program, e.g., a virus, that the database stores records of web pages which do not contain an executable program.

Second and third points of novelty are present in feature (b) which reads:

b) means for processing a file being transferred between computers, the means b) comprising:

> a file recogniser operative to determine whether the file being processed is an instance of a known program by checking the contents of the file being

> processed for the presence of said at least one characteristic signature associated with the said instances; and
> a difference checker operative, in the case that the file recognizer determines the file being processed to be an instance of a known program, to check whether the file is an unchanged version of that known program;

The first point of novelty discussed above that Roberts does not relate to detecting instances of "known programs" is also present in feature (b). Moreover, even assuming for the sake of argument, and without admission, that the disclosure in Roberts of a database of internet addresses of web pages which have been preemptively scanned and found not to contain malware is erroneously read onto feature (a), Roberts nonetheless fails to disclose all the recitations of feature (b) in combination.

Applicant and the Examiner appear to have a common understanding that Roberts discloses in paragraph [0034] the storage in the database of a checksum in respect of each internet address and that Roberts discloses in paragraph [0037] comparison of the stored checksum against the new checksum. The Examiner contends that this disclosure of Roberts reads onto feature (b) of claim 1, but Applicant respectfully disagrees for at least the following reasons.

A second point of novelty is that the recitation of "a file recogniser operative to determine whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances [emphasis added]" is novel. It is apparent from the Response to Arguments that the rejection is made on the basis that the checksum in Roberts reads onto the feature of claim 1 of "at least one characteristic signature associated with the said instances". However on this reading of Roberts, there is no disclosure of the feature of claim I of "checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances". Roberts compares the stored checksum with a checksum for the new web page. This is simply not checking the contents of the web page for the presence of a characteristic signature.

A third point of novelty is that feature (b) requires two separate elements of a file recogniser and a difference checker, the difference checker being operative selectively depending on the determination of the file recogniser. In Section 5 of the Office Action, the Examiner states that both the elements of a file recogniser and a difference checker lack novelty due to the same disclosure in Roberts of the comparison of checksums. However, this is incorrect because the single comparison of checksums cannot take away the novelty of both of the two elements recited in claim 1.

The prior response assumed that the comparison of checksums in Roberts was similar to the element of the difference checker of claim 1. In that case, Roberts has no disclosure of the element of the file recogniser, because the internet address stored in the database of Roberts does not meet the requirement of "to determine whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances". These arguments remain valid.

However, in the Response to Arguments and in Section 5 of the present Office Action, the Examiner takes the alternative position that the use of the checksum in Roberts reads onto the element of the file recogniser. Even if this were correct (which Applicant does not accept for the reasons discussed above with respect to the second point of novelty), then Roberts would not additionally disclose the element of a difference checker which is required to be operative when the determination of the file recogniser is that the file being processed is an instance of a known file.

A fourth point of novelty is feature (c) which reads:

> c) means for signalling the file, depending on the determination made by the processing means, as being:
> likely to be not malware if it is an unchanged version of a known file; likely to be malware if it is a changed version of a known file; or of unknown status if is not determined as being an instance of a known file.

Thus feature c) requires that the means is capable of signalling three different outcomes. This is similar to the second point of novelty because the two different

elements of feature b) are capable in combination of making three different determinations.

In Section 5 of the Office Action the Examiner states that this feature is disclosed in Roberts in paragraph [0038], lines 1-12. However this passage of Roberts discloses only two alternative determinations, namely (1) that the web page is unchanged, in which case it is supplied without scanning and (2) that the web page is changed, in which case it is scanned before being supplied. Therefore this passage of Roberts fails to disclose the entirety of feature (c) of claim I, which is therefore novel.

The other independent claims 7 and 13 contain similar recitations and are therefore novel for similar reasons.

Consequently, Applicants respectfully submit that claims 1, 2, 7, 8, 11 and 13-15 patentably distinguish over Roberts.

The remaining dependent claims 6, 12 and 16 are rejected based on proposed combinations of Roberts with Wu et al. (U.S. Patent No. 5,617,533) or Chao et al. (U.S. Patent Publication No. 2004/0128355). These other references do not remedy the deficiencies of Roberts with respect to the independent claims and thus Applicant submits that claims 6, 12 and 16 patentably distinguish over the combinations of art proposed in the office action.

The pending claims are believed to be allowable and favorable office action is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

Michael J. Shea
Reg. No. 34,725

MJS:mjs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100